Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Digital Broadcast Content Protection	)	MB Docket No. 02-230

ECHOSTAR SATELLITE LLC'S OPPOSITION TO NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION'S PETITION FOR RECONSIDERATION OR CLARIFICATION

EchoStar Satellite LLC ("EchoStar") hereby opposes the Petition for Reconsideration or Clarification submitted by the National Cable & Telecommunications Association ("NCTA") in the above-referenced matter, insofar as it asks the Commission to reconsider its definition of "demodulator" in the Broadcast Flag[1] rules to address a supposed disparate burden on cable equipment to comply with robustness and other requirements imposed by the rules. This misguided request should be rejected by the Commission because it is not necessary to enhance copy protection for direct broadcast satellite ("DBS") retransmission of digital broadcasts, and such a rule modification may in fact detract from the level of that protection.

To effectively comply with copyright law, DBS systems must encrypt the signals of local broadcast stations, and therefore the demodulator output for DBS services already conforms to robustness standards more rigorous than those imposed by the rules, obviating the

[1] *In the Matter of Digital Broadcast Content Protection*, Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd. 22940 (2003) ("*Broadcast Flag R&O*").

need for any additional protection.[2] Moreover, NCTA's request is inconsistent with the Commission's decision to give multichannel video programming distributors ("MVPDs") the latitude to "effectuate[] the flag's intent through their own conditional access system," "as appropriate for their distribution platforms."[3] NCTA's request detracts from that latitude by attempting to force all MVPDs to effectuate the flag in the same way, giving no consideration to what each platform's unique characteristics may dictate to achieve robust, efficient effectuation of the flag. The nature of EchoStar's system is such that the broadcast flag itself will not be transmitted, although the intent of the flag will be conveyed by EchoStar's conditional access system, consistent with the Commission's Report and Order. NCTA's uniformity request will lead to absolutely no enhancement in robustness or security, and will more likely result in increased costs and compromised content security. Accordingly, there is no reason to impose these requirements on QPSK, 8-PSK and successor (collectively "n-PSK") demodulators such as those used by DBS systems.[4]

Finally, EchoStar notes that an increasing portion of the set-top boxes it deploys contain both 8-VSB and n-PSK demodulators. The 8-VSB demodulators in those boxes will be in full compliance with the applicable rules, rendering NCTA's request even less relevant.

---

[2] Cable operators, on the other hand, must retransmit local stations (whether analog or digital) in the clear, which means that the rules' robustness requirements might be appropriate to preserve the protection of the broadcast flag for "QAM" cable demodulators. *See* 47 C.F.R. § 76.630.

[3] *Broadcast Flag R&O*, 18 FCC Rcd. 22940, ¶ 58.

[4] EchoStar notes that other transport systems, such as DOCSIS (used by cable modems) may also use n-PSK modulation. Thus, a blithe grant of NCTA's request to include n-PSK demodulators within the definition of "demodulator" for purposes of the rule could result in expansion of the broadcast flag obligations to DOCSIS boxes as well.

I. THERE IS SOUND JUSTIFICATION FOR THE DEFINITION TO COVER QAM DEMODULATORS AND NOT n-PSK DEMODULATORS

Devices that fall within the rule's definition of "demodulators" must comply with the rule's robustness and other requirements.[5] "Demodulators" are defined to include Quadrature Amplitude Modulation ("QAM") demodulators.[6] NCTA maintains that the rules "impose more burdens on cable operators than they do on their chief competitors, DBS providers," because this definition includes QAM demodulators which are used in cable set-top boxes, but not n-PSK demodulators, which are used in DBS boxes.[7] NCTA, however, overlooks a critical distinction between cable service and DBS service – DBS systems already conform to robustness standards more rigorous than those imposed by the rules upon cable retransmission of broadcast signals because DBS systems utilize encryption for *all* local signals.

Specifically, unlike cable systems, DBS providers already encrypt local signals to comply with the geographic restrictions on retransmission of such signals arising from copyright law.[8] The compulsory copyright license that allows satellite providers to retransmit a local broadcast signal to its local market extends only to the local "Designated Market Area" ("DMA") from which the signal originates.[9] Yet, because of the nature of satellite transmission, each local signal is beamed down to an area that is typically larger than the corresponding

---

[5] *See* Rules 73.9003, 73.9004 and 73.9007.

[6] *See* Rule 73.9000(g).

[7] *See* NCTA Petition for Reconsideration at 3-4.

[8] Cable operators, on the other hand, are generally prohibited from encrypting signals carried on the basic service tier, which includes local broadcast signals. *See* 47 C.F.R. § 76.630. *See also Broadcast Flag R&O*, 18 FCC Rcd. 22940, ¶ 59 (recognizing that cable operators are prohibited from encrypting the basic service tier and seeking comment on whether this rule should be modified for cable operators that retransmit digital television broadcasts).

[9] *See* 17 U.S.C. § 122(f).

DMA.[10] Satellite providers must therefore have in place a means of restricting reception of the local signal beyond the boundaries of the DMA. Source encryption is the means employed by DBS providers to control the reception of local signals.

Local signals, therefore, are never retransmitted by DBS systems in the clear. In fact, EchoStar uses the same level of encryption for local stations it retransmits that it does for basic and premium cable programming. This in turn means that broadcast content is subject to far more security in this DBS broadcast system than any protection that can be achieved by means of the broadcast flag. The superiority of systems such as that used by DBS was recognized by several commenters in the rulemaking proceeding, and was even suggested as a model for crafting content protection rules for digital broadcasts.[11]

Cable systems, on the other hand, must retransmit broadcast signals in the clear, and may reasonably be subjected to the robustness requirements that are intended to preserve whatever level of protection is afforded by the flag. In light of this critical distinction, it makes no sense to impose these requirements on DBS systems, which already utilize the most robust

---

[10] This is true even if the local station is transmitted on a spot beam, as the spot beam cannot be precisely focused to track the contours of the DMA, and typically covers wider areas.

[11] *See, e.g.*, Comments of Motorola (dated Dec. 6, 2002) at 5 ("source encryption is overwhelmingly accepted as mandatory among the professional security technology community. High value content distributed over satellite and cable has been analog scrambled or digitally encrypted since the 1980's, and broadcast DTV should be no exception to this well-established, well-justified convention."); Comments of Public Knowledge and Consumers Union (dated Dec. 6, 2002 at 12 ("the end-to-end scrambling systems of satellite and cable systems do not have the flaws of 'marking'-based copy-protection systems like the broadcast-flag proposal."). The superiority of source encryption was even recognized by broadcast flag proponents. *See* Comments of Digital Transmission Licensing Administrator LLC (dated Dec. 6, 2002) at 7 ("[f]rom a technical perspective, protection is most effective when applied at the source, such as distribution of content in an encrypted form.").

method of content protection available.[12] DBS systems already achieve the content protection goals of the rules, a fact implicitly recognized by the Commission's rules, and by the Commission's decision to allow MVPDs "the latitude to implement the flag as appropriate for their distribution system, whether it be through direct pass-through or by effectuating the flag's intent through their own conditional access system."[13]

II. COVERAGE OF DBS SYSTEMS WOULD BE SUPERFLUOUS AND COULD IMPOSE COSTS WITH ABSOLUTELY NO CORRESPONDING INCREASE IN CONTENT PROTECTION, AND INDEED, WITH THE RISK OF DECREASED PROTECTION

First of all, EchoStar notes that with respect to some of the rules, an extension of the requirement to include n-PSK demodulators would make little sense for the simple reason that those rules apply only to unencrypted ATSC digital broadcasts in the first place.[14] Specifically, the provisions of Rule 1909(c) concern only *unencrypted* digital broadcasts. DBS providers encrypt all broadcast retransmissions; thus, Rule 1909(c) should not apply to DBS providers for this reason alone.

Moreover, given the nature of DBS systems such as EchoStar's, extending Rule 1909(b) to such systems would be equally illogical. Rule 1909(b) requires MVPDs retransmitting digital broadcast signals in encrypted form to comply with robustness and output

---

[12] Another critical distinction between cable and DBS concerns the set-top boxes employed by each. While cable boxes typically contain only a QAM demodulator, the majority of DBS boxes currently contain only an n-PSK demodulator. On the other hand, an increasing proportion of DBS boxes contain an 8-VSB demodulator as well as an n-PSK demodulator. The 8-VSB demodulators in EchoStar's boxes will, of course, comply with the applicable rules.

[13] *Broadcast Flag R&O*, 18 FCC Rcd. 22940, ¶ 58.

[14] *See* Rule 76.1909(c).

restrictions if the broadcast flag is present in the EIT or the PMT.[15] The EIT and PMT are defined in accordance with ATSC broadcast standards and MPEG standards.[16] DBS systems were launched before those standards were complete, and might not use these structures. Moreover, the flag will not appear in EchoStar's transport stream precisely because, as noted above, EchoStar intends to comply with the rules by conveying the presence of the broadcast flag through other means via its conditional access system. The Commission has recognized that different MVPD platforms may most successfully effectuate the broadcast flag by using different means, and has accordingly given MVPDs the latitude to effectuate the flag in the manner most appropriate for their platforms. The Commission should not eliminate this latitude by adopting NCTA's argument.

Nor should the Commission be swayed by arguments that the rules should be imposed on DBS systems notwithstanding their superior content protection capability because DBS should be able to comply easily with the rules' less stringent security measures. Such arguments senselessly advocate MVPD "parity" for its own sake and overlook the fact that imposition of the requirements on DBS providers would yield absolutely no benefit and might even harm the cause of copy protection, while potentially imposing needless costs.

Simply put, from a technical perspective, the broadcast flag rules require demodulator output to be protected by encryption to preserve the robustness of the flag, something not currently done by cable systems retransmitting broadcast signals. But in DBS

---

[15] *See* Rule 76.1909(b) ("Where a multichannel video programming distributor retransmits Unencrypted Digital Terrestrial Broadcast Content in encrypted form, such distributor shall, upon demodulation of the 8-VSB, 16-VSB, 64-QAM or 256-QAM signal, inspect either the EIT or PMT for the Broadcast Flag. . . .").

[16] *See* Rule 73.9000(k) and (m).

systems, the signal is already encrypted at this point, meaning there is nothing to gain by imposing the rules on DBS systems.

If, for the sake of "parity," the Commission were to require n-PSK demodulators to handle the broadcast flag in precisely the same way as cable demodulators, needless costs and security risks would be incurred to do so. Because broadcast signals retransmitted by DBS are always encrypted, the broadcast flag would be encrypted as well and could not be "seen" per se. Extension of the rules to DBS boxes, however, might be interpreted by some to require the "wheel-spinning" process of implementing part of the MPEG decoder to decrypt the signal, recognize the flag, and then re-encrypt the signal. All of this would be done to achieve what DBS systems already do, namely, encrypt the signal at the point of demodulator output. The costs of implementing this encryption-decryption-reencryption process would net absolutely nothing in terms of increased security. Indeed, the only thing to be attained by requiring decryption of the signal as it travels through the demodulator is increased risk of compromising the system's security.

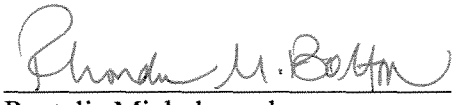
The source encryption employed by DBS systems already accomplishes the content protection goals of the broadcast flag rules, and indeed, protects content more vigorously than do the robustness requirements of the broadcast flag rule. Thus, there is no reason to subject DBS providers to the costs and the potential loss of security associated with any requirement that n-PSK demodulators function in the same way as cable demodulators. The Commission should decline any invitation to create "parity" for its own sake. However, if the Commission does elect to include n-PSK demodulators within the definition of covered demodulators under the rule, to avoid the imposition of needless costs and the potential compromise of DBS system security, the Commission should deem n-PSK demodulators, as they

currently function, to be in compliance with the robustness requirements of the broadcast flag rule.

III. CONCLUSION

For the foregoing reasons, NCTA's request to include n-PSK demodulators within the definition of demodulators covered by the broadcast flag rule should be rejected.

Respectfully submitted,



Pantelis Michalopoulos
Rhonda M. Bolton
Steptoe & Johnson LLP
1330 Connecticut Avenue NW
Washington, D.C. 20036
(202) 429-3000

Counsel for EchoStar Satellite LLC

Karen E. Watson
Lori Kalani
EchoStar Satellite LLC
1233 20th Street, NW
Washington, DC 20036

March 10, 2004

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Opposition to Petition for Reconsideration or Clarification was served this 10th day of March 2004 via U.S. mail, postage pre-paid, upon the following:

Daniel L. Brenner
National Cable & Telecommunications Association
1724 Massachusetts Avenue, NW
Washington, DC 20036

Lewis M. Bachman
Executive Director
The Songwriters Guild of America
1500 Harbor Blvd.
Weehawken, NJ 07086

Marvin L. Berenson
General Counsel
Broadcast Music, Inc.
320 West 57th Street
New York, NY 10019

Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street, NW, Suite 800
Washington, DC 20036
Counsel for Motion Picture Association of America, Inc.

Edward P. Murphy
President and CEO
National Music Publishers' Association
475 Park Avenue South, 29th Floor
New York, NY 10016

Terry G. Mahn
Fish & Richardson, P.C.
1425 K Street, NW
Suite 1100
Washington, DC 20005
Counsel for Genesis Microchip, Inc.

I. Fred Koenigsberg
White & Case LLP
1155 Avenue of the Americas
New York, NY 10036
Counsel for American Society of Composers, Authors and Publishers

Rhonda M. Bolton